

**UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	<b>Case No. 19-CR-00009-GKF</b>
<b>v.</b>	)	
	)	
<b>HONGJIN TAN,</b>	)	
	)	
<b>Defendant.</b>	)	

**TRIAL BRIEF OF THE UNITED STATES OF AMERICA**

The United States of America, through R. Trent Shores, United States Attorney, Joel-lyn A. McCormick and Matthew J. McKenzie, Assistant United States Attorneys for the Northern District of Oklahoma, respectfully submits its brief for trial in this case.

**I. STATUS OF THE CASE**

- a. TRIAL DATE: November 12, 2019, at 9:30 a.m., before the Honorable Judge Gregory K. Frizzell of the Northern District of Oklahoma.
- b. ESTIMATED TIME FOR TRIAL: 9 days.
- c. DEFENDANTS' STATUS: In Custody.
- d. WAIVER OF TRIAL BY JURY: None.
- e. INTERPRETER: No
- f. WITNESS LIST: As follows, dependent on stipulations.
  - 1. Employees of victim company
  - 2. Federal Bureau of Investigations Special Agents
  - 3. Federal Bureau of Investigation CART Team Members

4. Custodians of Records
5. Voluntary Informant.
- g. EXHIBIT LIST: As follows, depending on stipulations.
  1. E-mails
  2. Defendant's Employment Records
  3. Corporate Policies
  4. Forensic Data
  5. Documents executed and transmitted by e-mail
  6. Digital media collected and seized through the investigation
  7. Defendant's personal cell phone
  8. Defendant's personal laptop
  9. Defendant's company laptop

## **II. THE CHARGES IN THE INDICTMENT**

The Defendant is charged in Count One with a violation of 18 U.S.C. Section 1832(a)(1). This law makes it a crime to steal, appropriate without authorization, take or carry away trade secrets.

To find the defendant guilty of this crime you must be convinced that the government has proved beyond a reasonable doubt that:

1. The defendant knowingly stole, or without authorization appropriated, took, carried away, or concealed, or by fraud, artifice, or deception obtained information;
2. The defendant knew or believed this information was proprietary and he had no claim to it;

3. This information was in fact a trade secret;
4. The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;
5. The Defendant knew or intended that the offense would injure the owner of the trade secret; and
6. The trade secret was related to a product or service used or intended for use in interstate or foreign commerce.

The Defendant is charged in Count Two with a violation of 18 U.S.C. Section 1832(a)(2). This law makes it a crime to copy, transmit, or destroy a trade secret.

To find the defendant guilty of this crime you must be convinced that the government has proved beyond a reasonable doubt that:

1. The defendant knowingly, and without authorization, copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, or conveyed information;
2. The defendant knew or believed this information was proprietary and that he had no claim to it;
3. The information was, in fact, a trade secret;
4. The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;
5. The defendant knew or intended the offense would injure to owner of the trade secret; and
6. The trade secret was related to a product or service used or intended for use in interstate or foreign commerce.

The Defendant is charged in Count Three with a violation of 18 U.S.C. Section 1832(a)(3). This law makes it a crime to receive, buy, and possess trade secrets.

To find the defendant guilty of this crime you must be convinced that the government has proved beyond a reasonable doubt that:

1. The defendant knowingly, received, bought, or possessed information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
2. The defendant knew or believed this information was proprietary and that he had no claim to it;
3. The information was in fact a trade secret;
4. The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner of the trade secret;
5. The defendant knew or intended that the offense would injure the owner of the trade secret; and
6. The trade secret was related to a product or service used or intended for use in interstate or foreign commerce.

### **III. STATEMENT OF FACTS**

#### **A. Brief explanation of factual basis for each count**

On December 11, 2018, between 3:47 p.m. and 4:28 p.m., Tan accessed the Company database and stole trade secrets by placing them on a US Flash Drive.

On December 13, 2018, at approximately 11:01 a.m., Tan uploaded one of the trade secret documents to his personal cloud account.

On December 13, 2018, Tan also uploaded trade secret documents to a hard drive found in his apartment. The trade secret documents Tan placed on the external hard drive are the same five documents Tan stole from the Company on December 11, 2018 between 3:47 p.m. and 4:28 p.m. Tan continued to possess the external hard drive with the trade secrets until his arrest on December 20th, at which time agents executed a search warrant on Tan's residence and located the hard drive in his possession.

## **B. Overview of Background Information Leading to Indictment**

### **DESCRIPTION OF THE COMPANY**

Phillips 66 (“Company”) is a large international independent energy and petroleum corporation whose business focuses on exploration and development of petrochemical products and by-products and exploration and development of oil and natural gas. The Company’s technology is critical to its business.

The Company protects its proprietary technology and processes through a multi-layered strategy involving measures including physical security and password protected entrance into varied computer systems.

### **COMPANY’S PROPRIETARY TRADE SECRET INFORMATION**

The Company has a research facility in Bartlesville, Oklahoma, with its headquarters in Houston, Texas. The Company sold and shipped, and intended to sell and ship, a specified Research and Development Downstream Energy Market Product (“Product”). The Company researches, develops, and manufactures various energy sources in a city in Northern Oklahoma, and its facility there is used, in part, to research and develop the process used to manufacture the Product.

The Company earns revenue from its sale of the Product and multiple other proprietary products. The Company considers its methods of developing the Product to be trade secrets. The economic value of the Company’s methods of developing the Product is tremendously significant and of great value to competitors. The Company considers the Product as a source of revenue in the Company’s portfolio of global products. The Company’s annual revenue from the product is valued at millions of dollars.

### **HONGJIN TAN**

On April 21, 2017, the Company hired Hongjin Tan, a citizen of The People’s Republic of China (now a Legal Permanent Resident of the United States), as a research engineer in the battery development group in Bartlesville, Oklahoma. Among other things, Tan was responsible for research and development of the Company’s battery program operation, with the purpose of developing battery technology using the Company’s proprietary processes. Tan’s duties and responsibilities within the battery technology unit did not involve any work related to the Product at issue in this prosecution.

### **COMPANY’S DISCOVERY OF TAN’S THEFT**

On December 12, 2018, at approximately 10:30 a.m., Tan contacted his supervisor, Chris LaFrancois, and advised he was resigning from Company and was serving two

weeks' notice of his intent to resign from the Company. Tan told LaFrancois that he was returning to China to care for his aging parents. Tan told LaFrancois that he did not currently have a job offer, but was negotiating with a few battery companies in China. As a result, LaFrancois informed his supervisor, Kathy Woody, of Tan's resignation.

Tan's resignation prompted the Company to conduct a routine systems access review of Tan's computer activity. The review was conducted by the Company Information Technology (IT) Librarian, Laura Allen Ward.

After running a report to review Tan's access to Company research materials, Ward notified Woody of Tan's unusual research report access. The results of Tan's computer activity at the Company confirmed he had accessed files, including five reports unrelated to Tan's area of responsibility. The reports included not only how to make the Product, which, is a complicated and technically difficult process, but also the Company's plans for marketing the Product in China for specific clients. The files Tan accessed included information that the Company considered to be trade secrets. Ward's report indicated Tan last accessed the reports regarding the Product the day before he tendered his resignation.

Upon receiving information from Ward, Woody determined Tan posed a potential high-risk to the Company by being capable of possessing and/or revealing sensitive proprietary, trade-secret-protected information and decided to immediately escort him from the premises. At Woody's direction, LaFrancois located Tan and escorted him to LaFrancois' office, where they met with Woody. Woody told Tan he would not be allowed to come to the Company to finish his two weeks of employment, would be required to leave the Company property immediately, and would no longer have access to the Company's computer database or e-mail.

Woody permitted Tan to re-enter his office to take his personal bag and keys. Both of these items were searched by Woody and Company security prior to Tan's exit from the site. Tan's personal bag was a laptop knapsack. As part of the termination process, Woody completed an exit interview with Tan and required him to sign documents including a form certifying he did not have any Company property in his possession. Later the same day at approximately 4:00 p.m., Tan sent the following text message to LaFrancois' cell phone:

**“Hi Chris. This is Hongjin. Kathy was asking if there is anything I have with me associated with company IP. I have a memory disk that contains lab data that I plan to write report on, and papers/reports I plan to read at home. Now that I have been exited from (COMPANY), can you check what is the best way of handling the information and how sensitive they are? Can I still read the papers/reports from the memory disk?”**

After receiving the above text from Tan, LaFrancois asked Tan to deliver the USB Flash Drive (referred to by Tan as a “memory disk,” and referred to herein as “the USB Flash

Drive”) to the Company. Shortly after 5:00 p.m., Tan returned to the Company Research Technology Center where he delivered a USB Flash Drive to LaFrancois. The USB Flash Drive was Tan’s personal property, which he was not authorized to utilize within the Company’s space. There is no record of the Company having issued a USB Flash Drive to Tan.

After receiving the USB Flash Drive from Tan, LaFrancois immediately gave it to the Company’s Director of IT Shared Services, Dennis Betterton, for analysis.

### **EVALUATION OF POTENTIAL LOSS OF COMPANY’S TRADE SECRET INFORMATION**

Upon reviewing the USB Flash Drive, the Company IT Director Betterton determined the following:

- the USB Flash Drive that was in Tan’s possession outside of Company’s control contained data files that were owned solely by Company; and
- data on the USB Flash Drive, in deleted and undeleted files, contained research documents which would have a tremendous impact to Company in terms of technological and economic loss if they were to be shared or given to a competing company. Each page of the accessed document(s) was marked “confidential” and “restricted”.

During Betterton’s review, he identified files which were deleted from the USB Flash Drive on December 12, 2018. The deleted files remained on the USB Flash Drive in unallocated space. Company reviewed the deleted files (in addition to undeleted files on the USB Flash Drive) and determined that the deleted files included five reports. The Company conducted a Risk Assessment for the data. Company’s Risk Assessment included assigning the files “Technology Accessed Risk Levels.” Company assigned those files Technological Accessed Risk Levels ranging from Low-Medium to Extremely High. All of the deleted files were relevant to the Product, including one file that tracked the development of the Product over multiple decades.

The Company Risk Assessment also determined the disclosure of files relating to the Product found on unallocated space on the USB Flash Drive would allow the Company’s competitors and prospective competitors to manufacture the Product and would result in total erosion of the Company’s production of the Product.

By December 14, 2018, the Company ascertained Tan had accessed Company data over between 3:57 p.m. and 4:25 p.m. on December 11, 2018. According to Company IT specialists, Tan actually downloaded dozens of files to multiple thumb drives or other removable media. Tan did not report this access and was not granted authority by the

Company to download or remove data from the Company. Tan turned in the USB Flash Drive but did not turn in any other removable media onto which he downloaded proprietary information belong to the Company. In addition, on the one USB Flash Drive Tan did return to the Company, Tan had downloaded trade secrets and then deleted those trade secrets prior to delivering the USB Flash Drive to the Company. The deleted files were the same files referenced above as having been accessed between 3:57 p.m. and 4:25 p.m. on December 11, 2018.

Upon a search of Tan's residence on December 17, 2018, agents located a hard drive which also contained the same Product trade secret documents that had been uploaded to and subsequently deleted from the USB Flash Drive. Tan maintained possession of the hard drive after he delivered the USB Flash Drive to the Company. Tan never mentioned the fact that he uploaded the Product documents to a separate device. Based on a forensic analysis of the hard drive, the Product trade secret documents were last accessed on the hard drive on December 13, 2018.

Additionally, from a review of Tan's personal laptop, agents identified a cloud account belonging to Tan where one of the Product trade secret documents had been located on December 13, 2018 at 11:01 a.m. It cannot be determined whether third parties could or did access the cloud account. However, subscriber account information for the cloud account reflects that the account belonged to Tan and includes an address and telephone number known to be Tan's.

### **DESCRIPTION OF TAN'S CONTACT WITH COMPANY COMPETITOR**

On December 13, 2018, Tan had dinner with his former co-worker at the Company, Neal McDaniel. During this dinner, Tan told McDaniel he was leaving Oklahoma on December 27, 2018 to return to China. Contrary to what he told others in the Company, Tan told McDaniel that when he went to China in September 2018, he interviewed with a Chinese company and had been in constant contact with that company since he was in graduate school at The California Institute of Technology. The following day, McDaniel reported the conversation he had with Tan at dinner to Kathy Woody.

The Chinese company is Xiamen Tungsten Company, LTD. ("XTC") located in Xiamen, China. The company has "developed two production lines so far, one for Li-ion battery cathode materials (such as lithium cobalt oxide, ternary cathode material, lithium manganese oxide, lithium iron phosphate, etc.) and the other for NiMH battery anode material (Hydrogen storage alloy)." The company's profile description reflects its continuous effort to expand its portfolio and areas of production. Based on the company's profile, the Chinese company is considered a competitor of the Company in the area of energy development and technology. Although the Chinese company is now publicly traded it was once government owned.

### **TAN'S FOREIGN TRAVEL**

The government's evidence will include Tan's international travel records which confirm that on September 15, 2018, Tan traveled from the Dallas/Ft. Worth, Texas International Airport to Beijing,, China and returned to the United States on September 30, 2018.

### **PROTECTION OF COMPANY TRADE SECRETS**

The Company's methods of developing the Product were protected by the Company as confidential and proprietary information. The Company considers this information to be a trade secret, which was used in Product sells distributed in interstate or foreign commerce.

The Company used a number of reasonable measures to protect the Trade Secret Information and its other confidential proprietary information, including the following:

- the Company restricted access to the controlled environment in Oklahoma where the Product were conducted behind locked doors with magnetic card readers, and only certain employees were granted access;
- the Company limited access to the Trade Secret Information to those who needed it to perform their employment duties;
- the Company prohibited distribution of research products to other companies, persons, or countries for research;
- as a condition of their employment, the Company employees executed non-disclosure and assignment agreements, which specifically referenced the Company's confidential and proprietary information.

The Company implemented data security policies establishing that all information created, sent, received, or stored on the Company's electronic resources was company property and that all activity on the Company's electronic resources was subject to monitoring. These policies prohibited employees from transmitting, receiving, or storing company information outside the Company's electronic resources.

Tan was aware of the Company's measures to protect their Trade Secret Information due to the agreements he signed with the Company pertaining to confidential information, non-disclosure obligations, and intellectual property. Additionally, Tan, like all Company employees completed mandatory training annually. Part of the training Tan received addressed prohibitions against accessing restricted and confidential materials.

Additionally, on June 19, 2018, Tan signed a Confidential Information, Non-Disclosure and Intellectual Property Agreement which provided:

- without prior written consent of the Company, he would not “disclose, use, reproduce, or transmit (except for the performance of his duties for the Company), or permit the unauthorized disclosure, use, reproduction or transmission of any Confidential Information during the period of his employment with the Company or at any time thereafter”;
- he would not “upon leaving the employ” of the Company take with him any records, memoranda, drawings, pictures, models, papers, notebooks, reports, computer disks or other similar media having Confidential Information in or on such media.

Additionally, employees were reminded of their obligations to the Company when they would log in to his work computer. For example, when an employee of the Company begins to access their computer at work, the following warning appears on a screen banner before the employee can log in:

**This is a private computer system to be accessed and used for (Company) business purposes. By accessing, using and continuing to use this system or device, you agree to the terms of use. All access must be specifically authorized and used only in accordance with all applicable (Company) policies. Unauthorized access or use of this system is prohibited and may expose you to liability under criminal and civil laws. Absent a separate written agreement, all non-personal information and content you create, store or collect on behalf of (Company) or in the scope of your employment, on this computer system is the sole property of (Company). To the extent permitted under local law, (Company) reserves the right to monitor, access, intercept, records, read, copy, capture and disclose all information received, sent through or stored in this system or device, without notice, for any purpose and at any time.**

After a Company employee successfully logs into the Company’s computer systems, the exact same warning appears on the computer screen under the heading “**LEGAL NOTICE**”.

Additionally, the wording in a warning window described below appears anytime a Company employee activates the Company’s Virtual Private Network (VPN), which is a process which allows an employee to access the Company’s computer systems remotely:

**“When logging into Company network(s) you agree to comply with all applicable export control regulations. Further you agree you will not**

**access Company’s network from any countries subject to comprehensive U.S. Embargoes/Sanctions, including Cuba, Iran, North Korea, Sudan, or Syria.”**

**EMPLOYMENT OFFER FROM XIAMEN TUNGSTON (XTC).**

On December 19, 2018, Tan’s laptop computer that was issued to him by the Company was forensically examined by technically trained Federal Bureau of Investigation CART Team Specialist. During the review, a Chinese-language letter was located that had been scanned into the laptop.

This letter, bearing a stamped logo of Xiamen, was dated October 15, 2018. At the bottom of the letter was what appeared to be Tan’s signature and the date of October 17, 2018. An image of this letter was submitted to an FBI Chinese linguist who translated the text of the letter. The certified translation set out as follows:

The employment offer from the Chinese company was made following Tan’s September trip to China. During his exit interview, Tan provided personnel at the Company with false information, stating that he was returning to China to take care of his parents and he did not yet have employment, despite his offer of employment with the Chinese company. Tan covertly collected documents in reference to the Product as he planned to separate from the Company.

**IV. LEGAL ISSUES**

**A. Use of Charts**

**1. Generally**

It has long been the rule that charts may be exhibited to the jury during the trial in the discretion of the trial court in order that they “may guide and assist the jury in understanding and judging the factual controversy.” *United States v. Downen*, 496 F.2d 314, 321 (10th Cir. 1974); *See, United States v. Kaatz*, 705 F.2d 1237 (10th Cir. 1983); *United States v. Behrens*, 689 F.2d 154 (10th Cir. 1982). *See generally* Federal Rule of Evidence 1006. Of course, the jury should be instructed that the charts are not in and of themselves proof of any facts, and that if the charts do not correctly reflect facts or figures

shown by the evidence in the case, the jury should disregard the charts. *United States v. Skalicky, supra*; *United States v. Foshee, supra*; *United States v. Ellenbogen, supra*. The Second Circuit, in *United States v. Ellenbogen*, 365 F.2d 982 (2d Cir. 1966), *cert. denied*, 386 U.S. 923 (1967), allowed the admission of a chart that summarized other exhibits.

The court held that: The admission of charts is discretionary with the trial judge and is subject to review only on a clear showing of abuse and resulting prejudice to the opposing party . . . . The trial judge carefully cautioned the jury when [the summary] was admitted into evidence that the chart was only to assist them in understanding the figures and that where there was any conflict between the chart and the underlying data from which it was prepared, the underlying data would control. *Id.* at 988.

*See also: United States v. Kaatz, supra*; *Lloyd v. United States*, 226 F.2d 9, 16-17 (5th Cir. 1955); *United States v. Brickey*, 426 F.2d 680, 686-87 (8th Cir. 1970), *cert. denied*, 400 U.S. 828 (1970).

Thus, it is clearly within the discretion of the trial court to allow the use of charts at trial where they would be of assistance to the jury, subject to the appropriate limiting instructions, and such discretion will be subject to review only upon a clear showing of abuse and resulting prejudice to the opposing party. *United States v. Ellenbogen, supra* at 988; *Lloyd v. United States, supra* at 16.

Charts are used in opening statement to help explain to the jury what the case is about and to outline the proof that will be introduced. Of course, that is the precise function of an opening statement. *See, e.g., United States v. DeVincent*, 632 F.2d 147, 153 (1st Cir. 1980); *Government of Virgin Islands v. Turner*, 409 F.2d 102 (3d Cir. 1968);

*Foster v. United States*, 308 F.2d 751, 753 (8th Cir. 1962). Where a chart used to accompany an opening statement does no more than assist the jury in understanding the nature of the proof it is about to hear, use of the chart should be sustained. *See United States v. Churchill*, 483 F.2d 268, 274 (1st Cir. 1973); *United States v. Rubino*, 431 F.2d 284, 289-90 (6th Cir. 1970), *cert. denied*, 401 U.S. 910 (1971).

The use of charts in the opening statement and closing argument is governed by the same principles that apply to the use of charts at trial. *See United States v. Churchill, supra; United States v. Rubino, supra.* As described above, these aids will help the jury visualize the evidence. *Government of Virgin Islands v. Turner*, 409 F.2d at 103, and “to make it easier for the jurors to understand what is to follow, and to relate parts of the evidence and testimony to the whole,” *United States v. Dinitz*, 424 U.S. 600 at 612 (1976) (Burger, C.J., concurring).

Prior to permitting the United States to use the demonstrative aids, the court may caution the jury that the illustrations are only aids to assist the jury in understanding the case. Of course, certain charts are evidentiary in nature and are offered into evidence. The government understands that if a chart is offered as evidence, the Court must determine that they are based upon and fairly represent competent evidence before the jury. The Court’s cautionary instructions are important to ensure the jury understandings that the evidentiary value of the demonstrative aid depends entirely on the accuracy and credibility of the proof offered at trial upon which the charts are based. *See United States v. Downen, supra; United States v. Conlin*, 551 F.2d 534, 538 (2d Cir. 1977).

## **2. Summary Charts or Demonstrative Aids**

Summary charts may be utilized in two distinct manners. They may be used as “evidence summaries” or “educational devices” to summarize testimony or documents that have already been presented in court, , or they may be introduced as evidence themselves to prove the contents of voluminous writings that cannot be conveniently introduced and examined in court. *United States v. Behrens*, 689 F.2d at 161.

Historically, summary charts used as pedagogical devices have been allowed in the courtroom as an aid to the jury in cases involving complex or voluminous evidence. *See United States v. Downen*, 496 F.2d 314, 319 (10th Cir. 1974) (Blackboard “chart” allowed as demonstrative exhibit); *United States v. Alker*, 260 F.2d 135 (3d Cir. 1958) (summary chart made from documents and records in tax evasion case prepared and submitted by revenue agent); *United States v. Bartone*, 400 F.2d 459 (6th Cir. 1968), *cert. denied*, 393 U.S. 1027 (1969) (summary chart allowed to summarize defendant’s financial dealings in income tax evasion trial); *United States v. Swan*, 396 F.2d 883 (2d Cir. 1968), *cert. denied*, 393 U.S. 923 (1968) (summary of multiple count indictment allowed); *Gordon v. United States*, 438 F.2d 858 (5th Cir. 1971), *cert. denied*, 404 U.S. 828 (1971) (summary chart allowed to summarize evidence in misapplication of bank funds and falsifying records trial); *United States v. Churchill*, *supra* (summary charts used in misapplication of funds trial to illustrate steps in alleged fraudulent transactions); *United States v. Harenberg*, 732 F.2d 1507, 1513 (10th Cir. 1984) (use of summary in tax prosecution; Tenth Circuit has approved use of summaries in tax prosecutions on other occasions).

Prior to the adoption of Rule 1006 [of the Federal Rules of Evidence] the law governing the evidentiary status of summaries and therefore their use was unsettled. Striking

differences had developed within and among the circuits, no doubt causing the district courts to resort to various approaches in handling summaries at trial . . . Among the opinions treating summaries as evidence the more liberal school required no underlying documents to be received in evidence as a foundation for the summaries. All that was required was that the underlying documents be made available to opposing counsel for cross-examination purposes . . . The summaries were therefore given an independent evidentiary strength of the preparer's foundation testimony, thereby avoiding the need to receive voluminous documentary evidence at trial. Under the most restrictive view summaries were never accorded the position of evidence. Rather they were treated as jury aids designed to clarify voluminous documentary evidence already in the record and to provide a manageable perspective for the jury in its deliberations. Juries were not permitted to see the summaries unless every fact reflected was established by evidence in the record.

*United States v. Smyth*, 556 F.2d at 1183.

The enactment in 1975 of Federal Rule of Evidence 1006 resolved those uncertainties regarding the status of summaries. *Smyth*, 556 F.2d at 1184. Rule 1006 provides:

The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

The premise of Rule 1006 is that instead of using a summary chart, the proponent of the summary could have introduced the underlying documents upon which the summary is based. *See Smyth*, 556 F.2d at 1184 and n. 11. Summary charts which present an organization or summary to aid the jury in its examination of evidence already admitted

actually fall under the authority of Federal Rule of Evidence 611(a). *United States v. Scales*, 594 F.2d at 563-4.

The danger of permitting presentation of a summary of some of the evidence in a criminal case is plain. The jury might rely upon the alleged facts in the summary as if these facts had already been proved . . . or as a substitute for assessing the credibility of witnesses . . . This danger has led to the requirement of “guarding instructions” to the effect that the chart is not itself evidence but is only an aid in evaluating the evidence . . . Despite the danger, however, most summaries are routinely admitted.

*Scales* at 564 (citations omitted).

A summary chart is admissible under Rule 1006 only if all of the records from which it is drawn are otherwise admissible. *State Office Systems, Inc. v. Olivetti Corp. of America*, 762 F.2d 843, 845 (10th Cir. 1985). While the underlying materials must be “admissible,” they need not be “admitted” in every case. *United States v. Meyers*, 847 F.2d 1408, 1412 (9th Cir. 1988). Additionally, there is no necessity to examine the underlying records before a summary or chart may be utilized; the requirement is that the underlying “writings” be “voluminous” and that in-court examination not be convenient. *United States v. Scales*, 594 F.2d at 562. The underlying documents must also be available for inspection by opposing parties. *United States v. Kim*, 595 F.2d 755, 764 (D.C. Cir. 1979). See *R&R Associates, Inc. v. Visual Scene, Inc.*, 726 F.2d 36, 37-38 (1st Cir. 1984).

The decision to allow the use of summary charts is a matter within the trial court’s discretion, whether the charts are summaries of evidence previously admitted or summaries of voluminous documents or records which could have been admitted as evidence. See *United States v. Norton*, 867 F.2d 1354 (11th Cir. 1989), *cert. denied*, 491 U.S. 907 (1989);

*United States v. Pinto*, 850 F.2d 927; *State Office Systems v. Olivetti Corp. of America*, 762 F.2d 843 (10th Cir. 1985); *United States v. Downen*, 496 F.2d 314 (10th Cir. 1974); *United States v. Howard*, 774 F.2d 838 (7th Cir. 1985); *United States v. Behrens*, 689 F.2d at 154; *United States v. Nivica*, 887 F.2d 1110 (1st Cir. 1989), *cert. denied*, 110 S. Ct. 1300 (1990).

The Fifth Circuit conducted an analysis of these two different types of summary charts in *United States v. Smyth*, 556 F.2d at 1184. In *Smyth*, the government introduced two sets of computer printouts. The printouts summarized documents which had been admitted as evidence. When charging the jury, the court instructed that the printouts were not evidence but were only received as summaries of evidence. The Fifth Circuit stated that under Rule 1006, the district court could have properly excluded all of the underlying documents and received the summaries themselves as evidence. *Smyth* at 1184. Rule 1006 requires only the availability of the underlying documents. *Id.* In a subsequent case, almost 200 pages of material and substantial mathematical calculations were properly summarized in a chart which was admitted under Rule 1006. *United States v. Jennings*, 724 F.2d 436, 441 (5th Cir. 1984), *cert. denied*, 467 U.S. 1227 (1984). These particular charts also contained conclusions which were the product of assumptions by the government. “Such assumptions are allowed so long as supporting evidence has been presented previously to the jury . . . and where the court has made it clear that the ultimate decision should be made by the jury as to what weight should be given to the evidence.” *Jennings* at 442. See *United States v. Norton*, 867 F.2d at 1354. The witness preparing the chart in *Jennings* was subject to full cross-examination by the defendants and the trial court repeatedly cautioned the jury that the charts were the government's view of the

evidence. The defendant's contentions that an expert witness was required to prepare the present summary charts was also rejected. "When a chart does not contain complicated calculations requiring the need of an expert for accuracy, no special expertise is required in presenting the chart." *Jennings* at 443.

In a drug conspiracy case, the Ninth Circuit upheld the admission of summary charts which summarized long distance telephone call records and surveillance logs of two FBI teams. *United States v. Meyers*, 847 F.2d 1408 (9th Cir. 1988). At the time the chart was offered the telephone logs had been admitted and the head of one of the surveillance teams had testified fully. Later a member of the surveillance team testified. The surveillance logs had been made available for inspection by the defense but were never formally introduced into evidence. The court found that the surveillance reports, though not admitted, were admissible under Federal Rules of Evidence 803(6); and further that the defense was allowed, through cross-examination of the two agents who were members of the surveillance team, to alert the jury to any discrepancies in the chart. *Meyers* at 1412. Additionally, the sequence of events was confusing and the chart contributed to the clarity of the presentation. *Id.* See *United States v. Drougas*, 748 F.2d 8 (1st Cir. 1984) (summary charts admitted which pictorially summarized over 100 telephone calls placed during period of conspiracy).

Similarly, in *United States v. Possick*, 849 F.2d 332 (8th Cir. 1988), the court allowed the admission of charts summarizing roughly 250 telephone calls, and, twenty drug transactions memorialized by various hotel receipts and phone bills. In that case, demonstrative charts to aid in the jury's comprehension of the case were also admitted.

“Where charts which fairly summarize the evidence are used as an aid in understanding the testimony already introduced, and the witness who prepared the charts is subject to cross-examination with all the documents used to prepare the summary, the use of the charts is proper.” *United States v. Orlowski*, 808 F.2d 1283, 1289 (8th Cir. 1986), *cert. denied*, 482 U.S. 927 (1987); *see United States v. Caswell*, 825 F.2d 1228, 1235 (8th Cir. 1987); *United States v. Howard*, 774 F.2d 838, 844 (7th Cir. 1985); *United States v. Lemire*, 720 F.2d 1327, 1350 (D.C. Cir. 1983), *cert. denied*, 467 U.S. 1226 (1984); *United States v. Briscoe*, 896 F.2d 1476, 1495 (7th Cir. 1990), *cert. denied*, 111 S. Ct. 173 (1990).

In *United States v. Kapnison*, 743 F.2d 1450 (10th Cir. 1984), *cert. denied*, 471 U.S. 1015 (1985), charts which summarized the numerous government exhibits and testimony of witnesses were properly admitted. An agent testified as an expert in the area of tax matters and in so doing presented the charts. The jury was thoroughly instructed that the chart and the agent's summary of the evidence were not evidence but summaries of the evidence. Under these circumstances, the charts and summary testimony were proper. *Kapnison* at 1457. *See United States v. Mann*, 884 F.2d 532, 539 (10th Cir. 1989) and *United States v. Kaatz*, 705 F.2d 1237, 1245 (10th Cir. 1983).

The question of whether summary charts admitted under Federal Rules of Evidence 1006 may be sent to the jury was addressed by the Eighth Circuit in *United States v. Possick*, 849 F.2d 332 (8th Cir. 1988). The summary charts utilized by the government in that case (both summaries of voluminous documents and demonstrative devices) were permitted to go to the jury during deliberations. The Eighth Circuit opined that charts and diagrams admitted under Federal Rule of Evidence 1006 may be sent to the jury during

deliberations at the district court's discretion. *Possick* at 339; *see United States v. Orłowski, supra*. However, a limiting instruction is appropriate. *Id.* Additionally, the submission of purely demonstrative charts to the jury is disfavored and therefore limiting instructions are more strongly suggested. *Possick* at 339. *See also, United States v. Downen*, 496 F.2d at 314.

The size alone of a summary chart does not render the exhibit inadmissible if the evidence is otherwise unobjectionable objective evidence. *United States v. Behrens*, 689 F.2d at 162; *United States v. Scales*, 594 F.2d at 563. Additionally, the highlighting of some information on summary charts or the arrangement of names is not prejudicial so long as the court instructs the jury that the charts merely summarize the evidence, and that arrangement has nothing to do with culpability. *United States v. Porter*, 821 F.2d 968, 975 (4th Cir. 1987), *cert. denied*, 485 U.S. 934 (1988).

In the present case, the government will provide copies of any charts, diagrams or summary charts it intends to utilize in opening statement and/or its case-in-chief to defendant's counsel prior to trial. Of course, a summary chart intended for use in closing argument necessarily will be prepared on the basis of evidence admitted at trial and will be provided counsel prior to closing argument.

## **B. Chain of Custody**

### **1. Generally**

The test of admissibility of physical objects connected with the commission of a crime requires a showing that the object is in substantially the same condition as when the crime was committed or when the object was seized. Factors to be considered are the

nature of the article, circumstances surrounding its preservation and custody, and the likelihood of intermeddlers tampering with it. There is, however, a presumption of regularity in the handling of exhibits by public officials. *United States v. Wood*, 695 F.2d 459, 462 (10th Cir. 1982); *United States v. Kaiser*, 660 F.2d 724, 733 (9th Cir. 1981), cert. denied, 102 S. Ct. 1467 (1982).

A chain of custody indirectly establishes the identity and integrity of the evidence by tracing its continuous whereabouts. *United States v. Zink*, 612 F.2d 511, 514 (10th Cir. 1980). The criterion for admissibility is a showing that the physical evidence proffered is in substantially the same condition as when the crime was committed. *United States v. Wood*, 695 F.2d at 462; *Reed v. United States*, 377 F.2d 891, 893 (10th Cir. 1967); see also *United States v. Brown*, 482 F.2d 1226, 1228 (8th Cir. 1973). A court's determination that the showing as to identity and nature of the exhibit is sufficient to warrant the admissibility of it into evidence is reviewed for a clear abuse of discretion. *United States v. Wood*, 695 F.2d at 462; *United States v. Gagnon*, 635 F.2d 766, 770 (10th Cir. 1980), cert. denied, 451 U.S. 1018 (1981); *United States v. Zink*, 612 F.2d at 514; *United States v. Coleman*, 524 F.2d 593, 594 (10th Cir. 1975) (per curiam); *O'Quinn v. United States*, 411 F.2d 78 (10th Cir. 1969). Absent an abuse of discretion, deficiencies in the chain of custody go to the weight of the evidence and not its admissibility. See *United States v. Wood*, 695 F.2d at 462. See, e.g., *Reed v. United States*, 377 F.2d at 894, where the Tenth Circuit affirmed the trial court's finding of admissibility of certain evidence even though there were minor inconsistencies in the testimony. The court concluded that such inconsistencies go only to the weight accorded the evidence. *Id.*

Also, it is not necessary that the government establish all links in the chain of custody of an item or call all persons who were in a position to come in contact with it. See *United States v. Wood*, supra; *United States v. Kaiser*, supra; *Reyes v. United States*, 383 F.2d 734 (9th Cir. 1967).

### **C. Inextricably Intertwined Evidence**

In addition to predicate acts and overt acts the government will offer evidence which establishes the background and context of the charged crimes and which describes Tan relationship and involvement with employees and/or agents of the Chinese company. In particular, the government's evidence shows that after Tan made a trip to China in September 2018, he began assisting XTC with recruitment. The government will present evidence that Tan assisted XTC representatives in their completion of Visa applications. Although this evidence is not specifically described in the Indictment, it is admissible because it is inextricably intertwined with the evidence of the essential elements of the offenses charged. The Eleventh Circuit has defined inextricably intertwined evidence as follows:

Evidence, not part of the crime charged but pertaining to the chain of events explaining the context, motive and set-up of the crime, is properly admitted if linked in time and circumstances with the charged crime, or forms an integral and natural part of an account of the crime, or is necessary to complete the story of the crime for the jury.

Under the inextricably intertwined rubric, courts have admitted evidence of acts occurring prior to, during, and after the time periods set forth in the indictment. E.g., *United States v. Villareal*, supra (post-indictment acts); *United States v. Costa*, supra (pre-

indictment acts); *United States v. Aleman*, supra (acts during indictment time frame). This evidence has been admitted, for instance: (1) because it “pertained to a chain of events forming the context, motive and set-up of the crime” and, thus, was necessary “[t]o make the crime comprehensible to a jury,” *United States v. Mills*, 704 F.2d 1553 at 1559; accord, *United States v. Leichtman*, supra; *United States v. Hickey*, 360 F.2d 127 (7th Cir. 1966), cert. denied, 385 U.S. 928 (1966); (2) because it shows the relationship between co-conspirator witnesses and the defendants, *United States v. Richardson*, supra; *United States v. Costa*, supra; *United States v. Arias-Diaz*, 497 F.2d 165 (5th Cir. 1974), cert. denied, 420 U.S. 1003 (1975); (3) because it completed the story of the crime, *United States v. Aleman*, supra; *United States v. Bloom*, 538 F.2d 704 (5th Cir. 1976), cert. denied, 429 U.S. 1074 (1977); or (4) simply because it “tend[ed] to establish the conspiracy charged.” *United States v. Arias-Diaz*, supra; accord, *United States v. Villareal*, supra; *United States v. Angelilli*, 660 F.2d 23 (2d Cir. 1981), cert. denied, 455 U.S. 910 (1982).

#### **D. Admissibility of Electronically Transmitted Communications or Documents**

At trial, the government will seek to admit electronic evidence obtained during the course of the investigation. The electronic evidence includes e-mails, chat log printouts, and cloud account data obtained from the seized computers in this case. As set forth below, courts have held that this evidence is admissible under the Federal Rules of Evidence.

Primarily, the electronically stored evidence was obtained either through the execution of a search warrant, issuance of subpoena, or provided by the victim company.

The e-mails were obtained from Tan's personal and business e-mail accounts. The chat logs printouts were obtained from Tan's computers during the execution of the search warrants at residence and vehicle. In reviewing the evidence from the seized computer, the case agent printed out the e-mail and chat communications and other records.

### **E-Mails/Chat Communications and Other Electronically Stored Records**

As with other evidence, e-mails and chat log printouts and other records obtained from the seized computer are admissible where the requirements of the Federal Rules of Evidence are satisfied.

#### **1. Authentication**

The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Rule 901(a) only requires the government to make a *prima facie* showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification." Once the threshold showing has been met to admit the document, any questions concerning the genuineness of the item normally go to the weight of the evidence.

Through a number of established means, electronic evidence will be authenticated in this case, as noted below:

##### **a. By Witness With Knowledge**

As with other records, e-mails, chat communications and other records obtained from the seized computer may be authenticated under Fed. R. Evid. 901(b) by a witness with knowledge. For example, this permits authentication by a witness who participated

in the e-mail or chat communications. See, e.g., *United States v. Gagliardi*, 506 F.3d 389, 392-93 (2d Cir. 2007) (in prosecution for attempting to entice a minor to engage in prohibited sexual activity, e-mails and chat room communications between the defendant and a private citizen informant and undercover agent were authenticated by the informant and agent who “testified that the exhibits were in fact accurate records of Gagliardi’s conversations with” persons he knew as “Lorie” and “Julie”; fact that the e-mails and transcripts of instant-message chats were imported into another document, were not originals and could have been edited did not prevent admission; “a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable”); see also *United States v. Barlow*, 568 F.3d 215, 220 & n.17 (5th Cir. 2009) (trial testimony of other participant to chat conversation “could sufficiently authenticate the chat log presented at trial”); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (prima facie showing of authenticity established concerning chat room log printouts; witness “explained how he created the logs with his computer and stated that the printouts, which did not contain the deleted material, appeared to be an accurate representation of the chat room conversations among members of the Orchid Club”); see also *United States v. Safavian*, 435 F.Supp.2d 36, 40 n.2 (D.D.C. 2006) (noting e-mails between defendant government official and lobbyist could have been authenticated by recipient and sender but government chose not to call the lobbyist during trial).

b. By Agent

An agent familiar with the process used to obtain the e-mails, chat communications, and other records obtained from the seized computers will assist in authenticating these

records in this case. For example, a case agent will testify about the process used to obtain the computer records from the seized computers. *See, e.g., United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (in conspiracy to distribute marijuana case, a computer seized from one defendant's residence contained computer records of drug transactions and the drug business; rejecting argument that government was required to supply a witness with personal knowledge of the computer system; agent testimony authenticated the computer printouts under Rule 901(a) including that the computer was seized during the execution of a warrant, the agent was present when the computer records "were retrieved from the computer using the Microsoft Money program," and the agent "testified concerning his personal knowledge and his personal participation in obtaining the printouts"), *cert. denied*, 522 U.S. 1137 (1998).

The government plans to use "chain of custody" testimony to establish how the government obtained items located on the defendant's computers. *See, e.g., United States v. Salcido*, 506 F.3d 729, 733 (9th Cir. 2007) (per curiam) (in prosecution involving the possession and receipt or distribution of material involving the sexual exploitation of minors, "the government properly authenticated the videos and images under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers").

c. By Distinctive Characteristics

Under Fed. R. Evid. 901(b)(4), authentication may be made by distinctive characteristics, which may include "[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."

Courts have relied upon this rule in admitting e-mail and chat communications bearing distinctive characteristics. For example, this may include the e-mail addresses used in the communications, the context and circumstances, and other surrounding circumstances. See, e.g., United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (in fraud, false statements, and obstruction case, e-mail authenticated by contents and context, including e-mail address, automatic reply to sender, the messages indicated knowledge of matter, and use of nicknames; and foreign deposition testimony concerning phone conversations after e-mail messages were transmitted, applying Rule 901(b)(4)), cert. denied, 533 U.S. 940 (2001); *United States v. Safavian*, 435 F.Supp.2d 36, 40 (D.D.C. 2006) (e-mails between defendant government official and lobbyist were authenticated by distinctive characteristics under Rule 901(b)(4) including the e-mail addresses used which bore the sender's and recipient's names; "the name of the sender or recipient in the bodies of the e-mail, in the signature blocks at the end of the e-mail, in the 'To:' and 'From:' headings, and by signature of the sender"; and the contents).

A "hash value" or hash algorithm provides another accepted method to authenticate an electronic document by distinctive means. A hash value is commonly known as a "digital fingerprint." *See United States v. Henderson*, 595 F.3d 1198, (10th Cir. 2010) (noting a "SHA value serves as a digital fingerprint" and that "No two computer files with different content have ever had the same SHA value"). In this case, hash values were obtained as part of the pre- and post-examination process during the computer forensic examination. A computer forensics expert will testify how these measurements were made during the forensic examination process and the significance of these measurements.

Courts have used “hash values” as one means of authenticating electronic evidence. *See, e.g., Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 546-47 (D. Md. 2007) (“Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4).”); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 655 (D. Kan. 2005) (hash value “allows a large amount of data to be self-authenticating with a rather small hash mark, efficiently assuring that the original image has not been manipulated”).

d. By Comparison

Under Fed. R. Evid. 901(b)(3), authentication may be made by either the trier of fact or an expert.” Under this rule, the jury, as the trier of fact, may compare authenticated specimens with the evidence sought for admission. Some courts have used this rule to authenticate e-mails. *See, e.g., United States v. Safavian*, 435 F.Supp.2d 36, 40-41 (D.D.C. 2006) (e-mails between defendant government official and lobbyist were authenticated by comparing e-mail addresses, the use of the defendant’s name and business). In this case, there are e-mails, e-mail attachments, and chat communications which have been authenticated or are readily subject to authentication. The government will use these authenticated e-mails to authenticate other evidence obtained in the case.

**E. Available Witnesses Must Appear to Testify at Trial**

While the defense has not affirmatively stated its intent to offer deposition testimony at trial, the government includes this issue and controlling authority in its trial brief in support of its opposition to the deposition testimony being offered in lieu

of the deponents' appearances at trial. The inability to secure a witness's appearance must be considered under the specific provisions of Federal Rules of Evidence Rule 804 which provides as follows:

- (a) Criteria for Being Unavailable. A declarant is considered to be unavailable as a witness if the declarant:
  - (1) is exempted from testifying about the subject matter of the declarant's statement because the court rules that a privilege applies;
  - (2) refuses to testify about the subject matter despite a court order to do so;
  - (3) testifies to not remembering the subject matter;
  - (4) cannot be present or testify at the trial or hearing because of death or a then-existing infirmity, physical illness, or mental illness; or
  - (5) is absent from the trial or hearing and the statement's proponent has not been able, by process, or other reasonable means, to procure:
    - (A) the declarant's attendance, in the case of a hearsay exception under Rule 804(b) (1) or (6); or
    - (B) the declarant's attendance or testimony, in the case of a hearsay exception under Rule 804(b) (2), (3), or (4).

During a pretrial hearings, the defense has loosely claimed two XTC witnesses are unavailable for trial. Even after the government's urging, the defense did not describe any "exceptional circumstances" justifying a determination that the witnesses are unavailable. *Angelo v. Armstrong World Industries, Inc.*, 11 F.3d 957 (10<sup>th</sup> Cir. 1993).

Defense counsel has repeatedly represented that the witnesses are voluntarily making themselves available to be deposed. Defense counsel coordinated with counsel on behalf of the witnesses. The government has confirmed that both witnesses

applied for and currently possess active Visa's issued by The United States. Additionally, the government has confirmed that each witness has traveled to the United States on multiple occasions.

Given the deponents' willingness to testify, the defendant's ability to procure the witnesses attendance, and the witnesses history of traveling to the United States, there are no facts to support a finding that the witnesses are unavailable based on the criteria listed in Rule 804. Without a proper showing, the deponent witnesses must be made to appear to testify at trial.

**F. Government's Exhibits**

The United States will timely provide Defendants with a proposed exhibit list prior to trial. Consistent with standard practice in this Court, Counsels for the United States will seek to pre-admit all exhibits to facilitate the efficient presentation of evidence where no objections exist as to the chain-of-custody, relevance, or prejudicial nature of the evidence. The United States will work diligently with Defendant to address any evidentiary issues as they pertain to admission prior to the start of trial.

**V. CONCLUSION**

This brief is offered to acquaint the Court with factual and legal issues that may arise at trial. The United States requests that the Court grant leave to submit additional memoranda should other issues present later.

Respectfully submitted,

R. TRENT SHORES  
United States Attorney

/s/ Joel-lyn A. McCormick

JOEL-LYN A. McCORMICK, OBA #18240  
MATTHEW J. McKENZIE, NY Bar #4791513  
Assistant United States Attorneys  
110 West 7<sup>th</sup> Street, Suite 300  
Tulsa, Oklahoma 74119  
(918) 382-2700

**CERTIFICATE OF SERVICE**

I hereby certify that on the 1st day of November 2019, I electronically transmitted the foregoing document to the Clerk of Court using the ECF System for filing and transmittal of a Notice of Electronic Filing to the following ECF registrant:

Ryan A. Ray, Esq.  
[Rar@nwcjlaw.com](mailto:Rar@nwcjlaw.com)  
Attorney for Defendant

/s/ Joel-lyn A. McCormick  
Joel-lyn A. McCormick  
Assistant United States Attorney

CERTIFICATE OF DIGITAL SUBMISSIONS

I certify that all required privacy redactions have been made, and, with the exception of those redactions, every document submitted in digital form or scanned PDF format is an exact copy of the written document filed with the Clerk.

I also certify that the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Office Scan. I further certify that according to the commercial virus-scanning program, these digital submissions are free of viruses.

/s/ Joel-lyn A. McCormick

Joel-lyn A. McCormick  
Assistant U.S. Attorney